(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－106436

(43)公開日　平成８年(1996)４月23日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
G06F 15/00	330	B 9364-5L		

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）

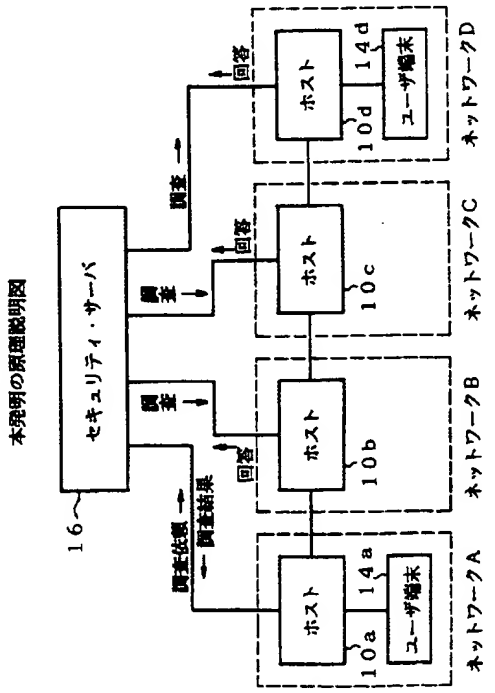
(21)出願番号　特願平6－238672

(22)出願日　平成６年(1994)10月３日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　田中　振一郎
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　竹内　進　（外１名）

(54)【発明の名称】広域ネットワークのユーザ認証装置

(57)【要約】
【目的】複数ネットワークのホストコンピュータを経由して不正利用しているユーザ端末を調査可能とする。
【構成】複数のネットワークＡ～Ｄに設けた各ホストコンピュータ１０ａ～１０ｄに対しセキュリティ・サーバ１６を接続し、各コンピュータ１０ａ～１０ｄからのユーザ調査依頼に対しセキュリティ・サーバ１６が他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末１４ｄを調査する。



1

【特許請求の範囲】

【請求項１】ホストコンピュータとユーザ端末を備えた複数のネットワークを相互に接続し、各ネットワークのユーザ端末から他のネットワークのユーザ端末にログインして情報を送受する広域ネットワークに於いて、

前記複数のネットワークに設けた各ホストコンピュータと接続し、各コンピュータからのユーザ調査依頼に対し他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末を調査するセキュリティ・サーバを設けたことを特徴とする広域ネットワークのユーザ認証装置。

【請求項２】請求項１記載の広域ネットワークのユーザ認証装置に於いて、前記各ネットワークのホストコンピュータは、他のネットワークを経由したユーザ端末からのログインに対し、前記セキュリティ・サーバにユーザ調査依頼を行い、該調査結果に基づいて前記ログインを許可又は拒否することを特徴とする広域ネットワークのユーザ認証装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、複数のコンピュータネットワークをお互いに結んだインターネットとして知られた広域ネットワークのユーザ認証装置に関する。

【０００２】

【従来の技術】従来、企業や大学の研究機関などのネットワークは、大型のホストコンピュータを中心に多数の端末機器を接続したローカルエリア・ネットワークとして構築されていたが、近年、このようなコンピュータネットワークをお互いに接続した広域ネットワークがインターネットとして急速に普及してきている。現在のところ、世界中の三百万台のコンピュータからなる３万のネットワークが存在するといわれ、これらのネットワークを相互に結合することで、極めて利用価値の高いネットワークが構築可能となる。

【０００３】図４は、広域ネットワークの一例であり、４つのネットワークＡ～Ｄを相互に結合しており、各ネットワークＡ～Ｄには、ホストコンピュータ１０ａ～１０ｄと、複数のユーザ端末が設けられる。そして、インターネットとしてネットワークＡ～Ｄを相互に結合することで、例えばネットワークＤのユーザ端末１４ｄからネットワークＣ，Ｂを経由してネットワークＡのユーザ端末１４ａにログインして、情報のやり取りを行うことができる。

【０００４】

【発明が解決しようとする課題】ところで、インターネットとしての広域ネットワークを構築した場合、他のネットワークからの通信要求を全て受け入れると、ネットワーク内部での情報のやり取りが制限される。そこで、各ネットワークにあっては、他のネットワークからログイン可能なユーザ端末の数に制限を加える場合がある。

2

【０００５】またネットワークによっては、特定のユーザ端末の情報については有料とする場合もあり、この場合には、ユーザＩＤを知って課金処理を行うことになる。このため広域ネットワークの中でコンピュータを運用していくに当っては、セキュリティの強化が重要になる。しかし、広域ネットワーク上で特定のネットワークに不正にログインしようとするユーザ端末が、他の複数のネットワークを経由して侵入してきた場合、どこのネットワークのユーザ端末から侵入して来たかの追跡は、現状では不可能に近いという問題がある。

【０００６】例えば図５のように、ネットワークＤのユーザ端末１４ｄからネットワークＡのユーザ端末１４ａに不正にログインを行ったとする。このログインは、ネットワークＤ～Ａのホストコンピュータ１０ｄ，１０ｃ，１０ｂ，１０ａを経由して来る。このユーザ端末１４ａに対するログインが不正利用と判っても、ホストコンピュータ１０ａへのログインは、ネットワークＢのホストコンピュータ１０ｂに接続している仮想的なユーザ端末１４ｂからのログインとしてしか見えず、ネットワークＣからのログインであることは判らない。同様にネットワークＢのホストコンピュータ１０ｂから見たログインは、ネットワークＣのホストコンピュータ１０ｃに接続している仮想的なユーザ端末１４ｃからのログインとしてしか見えず、ネットワークＤからのログインであることは判らない。

【０００７】この場合、ホストコンピュータ１０ａからホストコンピュータ１０ｂ，１０ｃに、ユーザ端末との接続状況を問い合せればよい。しかし、ホストコンピュータ１０ｂ，１０ｃは各々が独立した固有のネットワークＢ，Ｃを構築しているため、ホストコンピュータ１０ａからの問い合せに協力的であるとは限らない。このため複数のネットワークのホストコンピュータを経由した不正なログインは、現在の広域ネットワークでは調べようがなく、不正なログインをそのまま見逃してしまう問題がある。

【０００８】本発明は、このような従来の問題点に鑑みてなされたもので、複数ネットワークのホストコンピュータを経由して不正利用しているユーザ端末を調査して必要な措置がとれるようにした広域ネットワークのユーザ認証装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】図１は本発明の原理説明図である。まず本発明は、ホストコンピュータ１０ａ～１０ｄとユーザ端末１４ａ，１４ｄを備えた複数のネットワークＡ～Ｄを相互に接続し、各ネットワークのユーザ端末から他のネットワークのユーザ端末にログインして情報を送受する広域ネットワークを対象とする。

【００１０】このような広域ネットワークのユーザ認証装置として、本発明にあっては、複数のネットワークＡ～Ｄに設けた各ホストコンピュータ１０ａ～１０ｄと接

続し、各コンピュータ１０ａ～１０ｄからのユーザ調査依頼に対し他のホストコンピュータのユーザ接続情報を参照して発信元のユーザ端末１４ｄを調査するセキュリティ・サーバ１６を設けたことを特徴とする。

【００１１】ここで、各ネットワークＡ～Ｄのホストコンピュータ１０ａ～１０ｄは、他のネットワークを経由したユーザ端末からのログイン、例えばネットワークＣ，Ｂを経由したネットワークＤのユーザ端末１４ｄからネットワークＡのホストコンピュータ１０ａへのログインに対し、セキュリティ・サーバ１６にユーザ調査依頼を行い、調査結果に基づいてログインを許可又は拒否する。

【００１２】

【作用】このような本発明の広域ネットワークのユーザ認証装置によれば、複数のネットワークを経由したログインの情報を、各ホストコンピュータの上位に位置するセキュリティ・サーバで参照することで、ネットワークを越えて不正にログインしているユーザ端末装置を認識することができ、広域ネットワークのセキュリィを高めることができる。

【００１３】

【実施例】図２は、本発明のユーザ認証装置が適用される広域ネットワークの一例である。図２において、この実施例にあっては、４つのネットワークＡ，Ｂ，Ｃ，Ｄで広域ネットワークを構成している。即ち、ネットワークＡ～Ｄのそれぞれにはホストコンピュータ１０ａ，１０ｂ，１０ｃ，１０ｄが設けられ、ホストコンピュータ１０ａ～１０ｄは、お互いに通信回線１２で接続されている。

【００１４】ここで、ホストコンピュータ１０ａ～１０ｄを通信回線１２で直列接続しているが、これは図示の都合であり、実際にはホストコンピュータ１０ａ～１０ｄが相互に通信回線１２で接続されている。ホストコンピュータ１０ａ～１０ｄのそれぞれには、ネットワーク内部のローカルエリア・ネットワークによって複数のユーザ端末が接続されている。

【００１５】ネットワークＡ～Ｄ内でのユーザ端末間の通信は、例えばネットワークＡを例にとると、ユーザ端末１４ａが、ネットワーク内の他のユーザ端末に対する通信のためホストコンピュータ１０ａに対し予め定めたパスワードとユーザＩＤを送ることでログインすることができる。このログインにあっては、発信元となるユーザ端末１０ａより、相手先を示すユーザＩＤが同時に送られる。

【００１６】一方、異なるネットワークのユーザ端末間での通信については、その間に存在する複数のホストコンピュータを経由したログインが行われる。例えば、ネットワークＤのユーザ端末１４ｄからネットワークＡのホストコンピュータ１０ａにログインしてユーザ端末１０ａと通信したい場合には、ユーザ端末１４ｄからホストコンピュータ１０ｄに対するログイン、ホストコンピュータ１０ｄからホストコンピュータ１０ｃに対するログイン、ホストコンピュータ１０ｃからホストコンピュータ１０ｂに対するログインを経て、ホストコンピュータ１０ａに対するログインが行われる。

【００１７】この場合、ユーザ端末１０ｄはネットワークＡのホストコンピュータ１０ａについて定められたパスワードと自分自身のユーザＩＤを送ってログインを行う。ユーザ端末１０ｄからのログインに基づくホストコンピュータ１０ｄからホストコンピュータ１０ａへのログインの伝送は、ユーザ端末１４ｄが発信したパスワードを解析して、ネットワークＡに対するログインであることを認識して、次のネットワークのホストコンピュータに送り出すようになる。したがって、ネットワークＤとネットワークＡの間に存在するネットワークＣ，Ｂのホストコンピュータ１０ｃ，１０ｂには、ログインが行われたユーザ端末１０ｄからの送信情報が記録保持されている。

【００１８】このような４つのネットワークＡ～Ｄのホストコンピュータ１０ａ～１０ｄに対しては、共通にセキュリティ・サーバ１６が接続される。セキュリティ・サーバ１６は、ホストコンピュータ１０ａ～１０ｄからのログインしてきたユーザ端末に関する調査依頼を受けると、調査対象となったユーザ端末の発信元から発信先の間に位置するネットワークのホストコンピュータに対し、調査対象となったユーザ端末に関する調査を依頼する。具体的には、ホストコンピュータに対し、調査対象となっているユーザ端末のパスワードとＩＤコードを提供して、その通信記録を読み出して回答させる。

【００１９】例えば図２のように、ネットワークＤのユーザ端末１４ｄよりネットワークＡのホストコンピュータ１０ａがログインを受けた場合、この外部からのログインが、どのネットワークのユーザ端末によるものか判らないことから、ホストコンピュータ１０ａはセキュリティ・サーバ１６に対し、ログインしたパスワードとユーザＩＤを指定したユーザ端末の調査を依頼する。

【００２０】ホストコンピュータ１０ａからの調査依頼を受けたセキュリティ・サーバ１６は、他の全てのホストコンピュータ１０ｂ，１０ｃ，１０ｄに対しパスワードとユーザＩＤを提供し、調査を依頼する。セキュリティ・サーバ１６からの調査指示を受けたホストコンピュータ１０ｂ～１０ｄのそれぞれは、その通信記録を読み出してセキュリティ・サーバ１６に回答する。

【００２１】具体的には、ホストコンピュータ１０ｂは、調査対象となったパスワードおよびユーザＩＤのユーザ端末はネットワークＣのホストコンピュータ１０ｃからのログインであることを回答する。またホストコンピュータ１０ｄは、調査対象となったパスワードおよびユーザＩＤのログインはネットワークＤのホストコンピュータ１０ｄからのログインであったことを回答する。

更にホストコンピュータ１０ｄは、調査対象となったパスワードとユーザＩＤのログインは自分のネットワーク内のユーザ端末１０ｄからのログインであったことを回答する。

【００２２】このようなホストコンピュータ１０ｂ～１０ｄからの調査指示に対する回答結果をセキュリティ・サーバ１６で解析すると、ホストコンピュータ１０ａから調査依頼があったパスワードとユーザＩＤのログインは、ネットワークＤのユーザ端末１４ｄから行われたものであることが判り、この調査結果をホストコンピュータ１０ａに回答する。これによって、ホストコンピュータ１０ａ側において、調査対象としたログインがネットワークＤのユーザ端末１４ｄから行われていることを認識できる。

【００２３】一方、セキュリティ・サーバ１６による追跡調査でユーザ端末が突き止められず、追跡不能との調査結果の回答を受けた場合には、ホストコンピュータ１０ａにおいて、調査対象としたユーザ端末のログインを拒否することもできる。図３は、図２の各ホストコンピュータ１０ａ～１０ｄにおけるセキュリティ・サーバ１６を利用したセキュリティ処理のフローチャートである。

【００２４】まずステップＳ１で、必要があれば、調査対象となるユーザＩＤを予め設定しておく。この調査対象のユーザＩＤの設定状態で、ステップＳ２でログインをチェックしており、ログインがあると、ステップＳ３で、パスワードとユーザＩＤをチェックし、ステップＳ４で、調査対象として設定したユーザか否かチェックする。

【００２５】ログインしてきたユーザが調査対象として設定したユーザであった場合には、ステップＳ５で、セキュリティ・サーバ１６に対しパスワードとユーザＩＤを通知して、ユーザ端末の調査を依頼する。この調査依頼を受けて、セキュリティ・サーバ１６は他のホストコンピュータに調査を指示し、その回答から調査対象となったユーザ端末の追跡結果を報告してくる。この調査結果は、ステップＳ６で受信される。

【００２６】調査結果からユーザ端末が追跡できていた場合には、ステップＳ７からステップＳ８に進み、調査したユーザＩＤをもつユーザ端末を記録し、ユーザ端末が判っていることから、ステップＳ９で、ログインを受領する。また、調査したユーザ端末が不正使用であった場合には、ステップＳ８の記録結果を利用して、追跡したユーザ端末の不正使用に対し必要な措置をとることができる。

【００２７】一方、ステップＳ７で、受信した調査結果からユーザ端末が追跡不能であった場合には、ステップＳ１０で、ログインを拒否する。即ち、セキュリティ・サーバ１６で追跡不能のようなユーザ端末は、本来、不正使用を意図していることが明らかであることから、ログイン自体を拒否して不正使用を行わせないようにする。

【００２８】尚、上記の実施例は４つのネットワークを例にとるものであったが、ネットワークの数は必要に応じて適宜に設けられる。また、セキュリティ・サーバを４つのネットワークに対し共通に設けているが、ネットワークの数が増加した場合には、複数のネットワーク単位に共通に１つのセキュリティ・サーバを設け、複数設けられたセキュリティ・サーバ相互間でネットワークすることで、全体的なセキュリティ・サーバとしての機能を実現してもよい。

【００２９】

【発明の効果】以上説明してきたように本発明によれば、各ネットワークのホストコンピュータに対し共通にセキュリティ・サーバを設けたことで、複数のホストコンピュータを経由してログインしてきたユーザ端末に対し、各ネットワークのホストコンピュータ間の独立を保ちながら、発信元となったユーザ端末を認識することができ、複数のネットワークを経由することで、不正使用を行おうとしても、不正使用を行っている発信元が追跡されることで、不正使用を確実に把握でき、広域ネットワークのセキュリティを大幅に強化することができる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明の実施例を示したブロック図

【図３】本発明のセキュリィ処理のフローチャート

【図４】従来装置のブロック図

【図５】不正ログインに対する問題の説明図

【符号の説明】

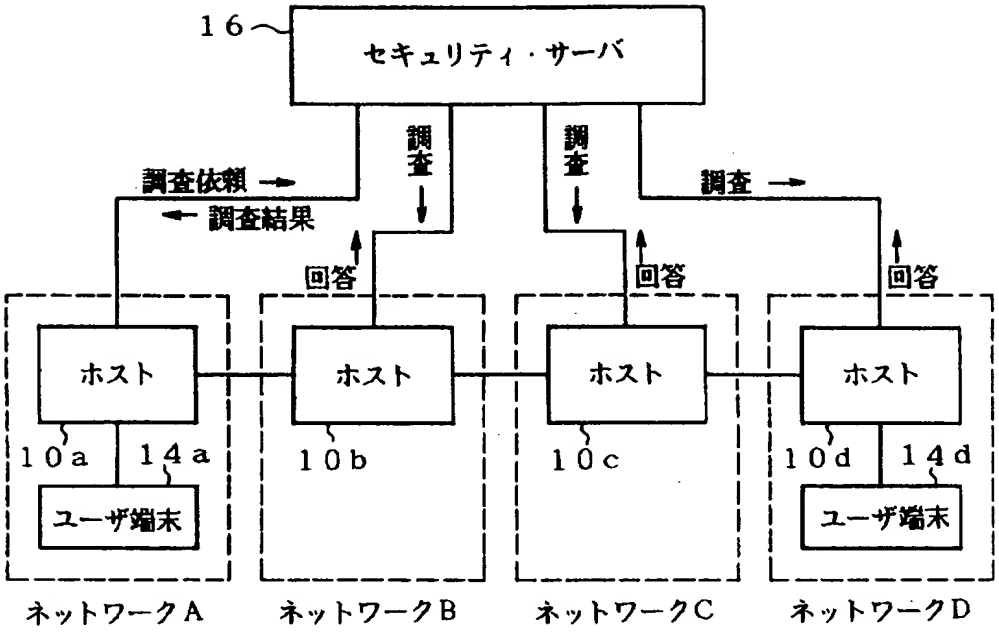
１０ａ～１０ｄ：ホストコンピュータ

１２：通信回線

１４ａ，１４ｄ：ユーザ端末

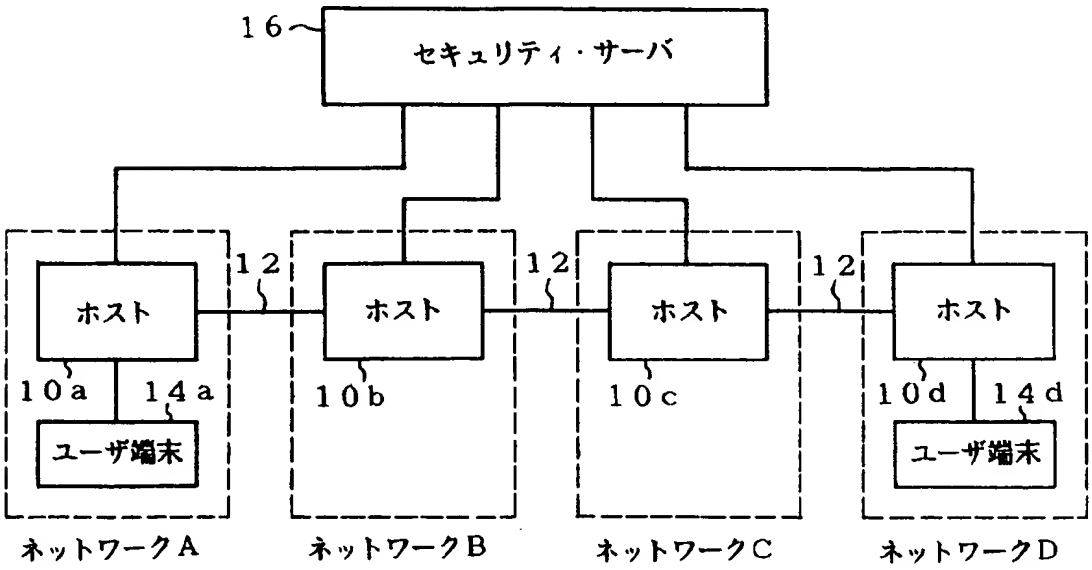
【図１】

本発明の原理説明図



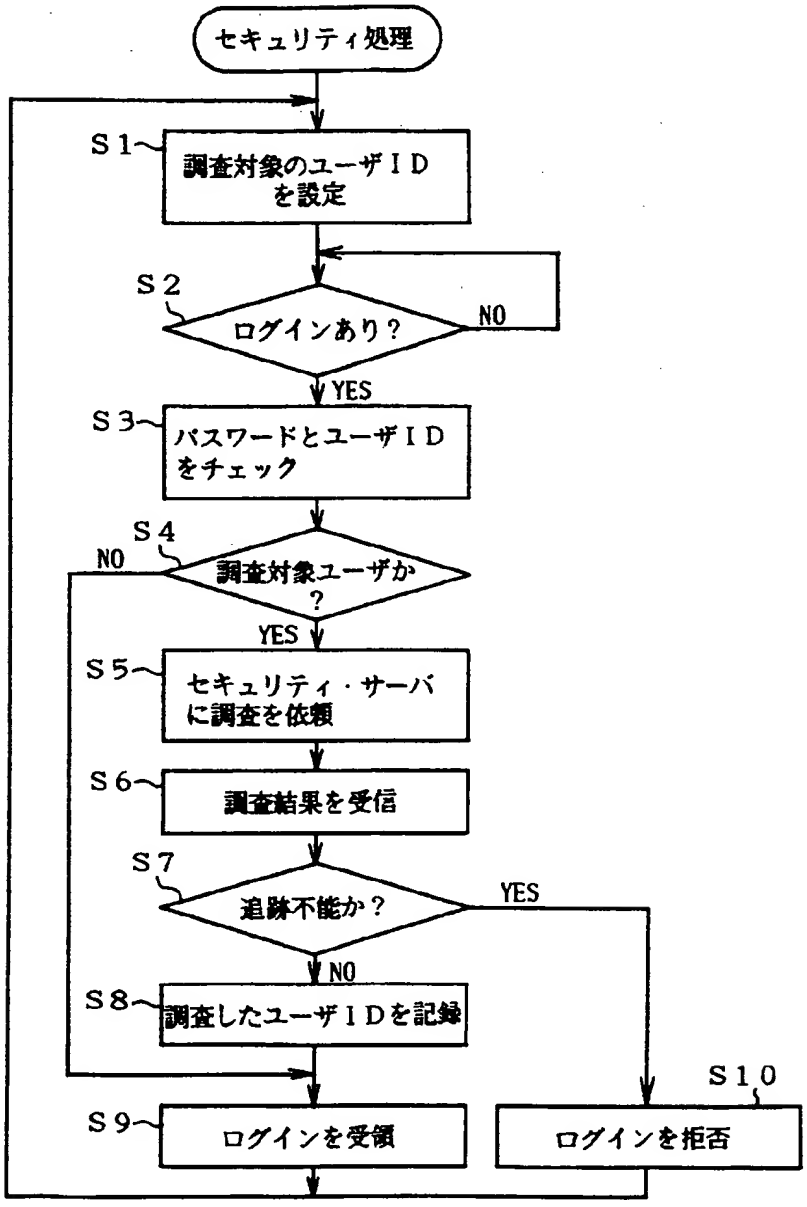
【図２】

本発明の実施例を示したブロック図



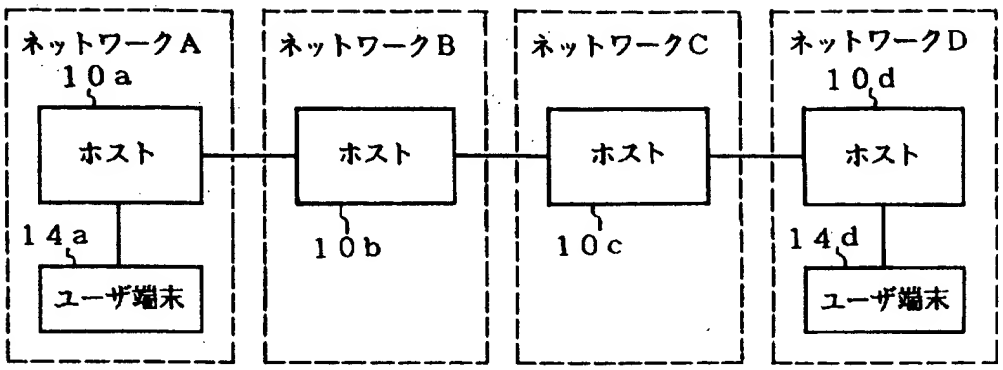
【図３】

本発明のセキュリィ処理のフローチャート



【図４】

従来装置のブロック図



【図５】

不正ログインに対する問題の説明図